

WHAT IS CLAIMED IS

1. A block-level storage device, comprising:
5 a storage medium; and
a storage engine, the storage engine being configured to generate a secure session key and to receive a block of encrypted content and its corresponding encrypted content key from a host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being
10 further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium.
2. The block-level storage device of claim 1, wherein the storage engine is
15 further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system.
3. The block-level storage device of claim 2, wherein the storage engine is
20 further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure session key only by decrypting the encrypted secure session key using the private key corresponding to the public key.

4. The block-level storage device of claim 3, wherein the storage engine is further configured to re-encrypt the block of encrypted content using at least a second storage engine encryption key.
- 5 5. The block-level storage device of claim 4, wherein the second storage engine encryption key comprises a Data Encryption Standard (DES) key.
6. The block-level storage device of claim 5, wherein the DES key comprises a triple DES key.
- 10 7. The block-level storage device of claim 1, wherein the storage engine is a hard disc storage engine and wherein the storage media is a hard disc.
8. The block-level storage device of claim 7, wherein the storage media is a
15 removable hard disc.
9. The block-level storage device of claim 3, wherein the public key and the private key are elliptic curve cryptography keys.
- 20 10. The block-level storage device of claim 1, wherein the storage engine includes a random number generator for generating the secure session key.
11. A method of writing to a block-level storage device from a host system having a public key and a corresponding private key, comprising:
25 encrypting a secure session key using the public key;

recovering the secure session key from the encrypted secure session key
using the corresponding private key;

encrypting content according to a content key and commanding the block-
level storage device to write the encrypted content to host-system-determined

5 block addresses;

encrypting the content key using the secure session key and transmitting the
encrypted content key to the block-level storage device; and

in the block-level storage device, decrypting the encrypted content key
using the secure session key.

10

12. The method of claim 11, further comprising:

in the block-level storage device, encrypting the decrypted content key with
a storage device key; and

writing the storage-device-encrypted content key to a host-system-

15 determined block address.

13. The method of claim 11, wherein the content comprises a file system
object, the method further comprising:

in the block-level storage device, encrypting the decrypted content key with

20 a storage device key, and

writing the storage-device-encrypted content key to a storage-device-
determined block address.

14. A system, comprising:

a host system, the host system configured to request for file system objects stored by a storage device by identifying the block addresses containing a requested file system object and requesting the storage device to return the content stored at the identified block addresses, the host system being further configured to
5 identify the file system object to the storage device if the requested file system object comprises secure content; and

a storage device having:

a storage medium configured to store security metadata for the secure file system objects; and

10 a storage engine, the storage engine being configured to respond to block-level requests from the host system by retrieving the content stored at the requested block addresses from the storage medium, the storage engine being further configured to access the security metadata if the block-level requests correspond to content comprising a secure file system object.

15

15. The system of claim 14, wherein the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system object content if the locking indicator indicates the file system object is locked.

20

16. The system of claim 15, wherein the storage engine is configured to change the security metadata for a secure file system object in response to an Internet transaction with a validated host system.

17. The system of claim 14, wherein the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host
5 system has no remaining play rights.

18. The system of claim 17, wherein the storage engine is configured to erase the security metadata if the play flag indicates that the host system has no remaining play rights.

10

19. The system of claim 17, wherein the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system object content if the locking indicator indicates the file system object is locked, and wherein the storage engine is configured to assert the
15 locking indicator if the play flag indicates that the host system has no remaining play rights.

20. The system of claim 14, wherein the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the
20 corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights.

21. The system of claim 20, wherein the storage engine is configured to modify security metadata for a secure file system object through an Internet transaction with an authorized host system.

5 22. The system of claim 14, wherein the storage engine is configured to generate a secure session key, the storage engine generating the security metadata for each secure file system object by receiving a corresponding encrypted content key from the host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to
10 decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium.

23. A system, comprising:
15 a host system, the host system being configured to request for non-secure file system objects by identifying the block addresses corresponding to the non-secure file system object and to request for secure file system objects by identifying the file system object; and
a storage device having:
20 a storage medium configured to store security metadata for the secure file system objects; and
a storage engine, wherein the storage engine is configured to control the file system used to store secure and non-secure file system objects on the storage medium, the storage engine being further configured to respond to block-
25 level requests for non-secure file system objects by translating the block-level

requests from the host system to byte-level offsets within a file system object on the storage medium, the storage engine being further configured to control the file system associated with secure file system objects by determining where secure file system objects will be stored on the storage medium and where the corresponding security metadata will be stored on the storage medium.

24. The system of claim 23, wherein the storage engine is a hard disc storage engine and wherein the storage media is a hard disc.

25. The block-level storage device of claim 24, wherein the storage media is a removable hard disc.

26. The system of claim 23, wherein the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system object content if the locking indicator indicates the file system object is locked.

27. The system of claim 23, wherein the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights.

28. The system of claim 23, wherein the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the

corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights.

- 5 29. A block-level storage device, comprising:
- a storage medium; and
- a storage engine, the storage engine being configured to respond to block-level non-secure content requests, block-level secure content requests, and block-level security metadata requests from a host system, the storage engine being
- 10 further configured to, in response to a security metadata request, generate a secure session key and to receive an encrypted content key from the host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a
- 15 first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium.

30. The block-level storage device of claim 29, wherein the storage engine includes a random number generator for generating the secure session key.

20

31. The block-level storage device of claim, wherein the storage engine is configured to receive a public key from the host system and to encrypt the secure session key with the public key and to send the encrypted secure session key to the host system, whereby the host system may recover the secure session key only
- 25 through the use of the host system's corresponding private key.